KRIPTOGRÁFIA

Varga Felicián
gazdaságinformatikus
WVG-883

TARTALOM

- A kriptográfia fogalma
- A kriptográfia története
- A kommunikáció folyamata
- A kriptográfia részei
- A szöveg útja
- A jó titkosítás ismérvei
- Caesar féle titkosítás
- Caesar féle kulcsszavas titkosítás
- Polybios féle titkosítás
- Egyéb titkosítási módszerek
- RSA algoritmus
- Digitális aláírás

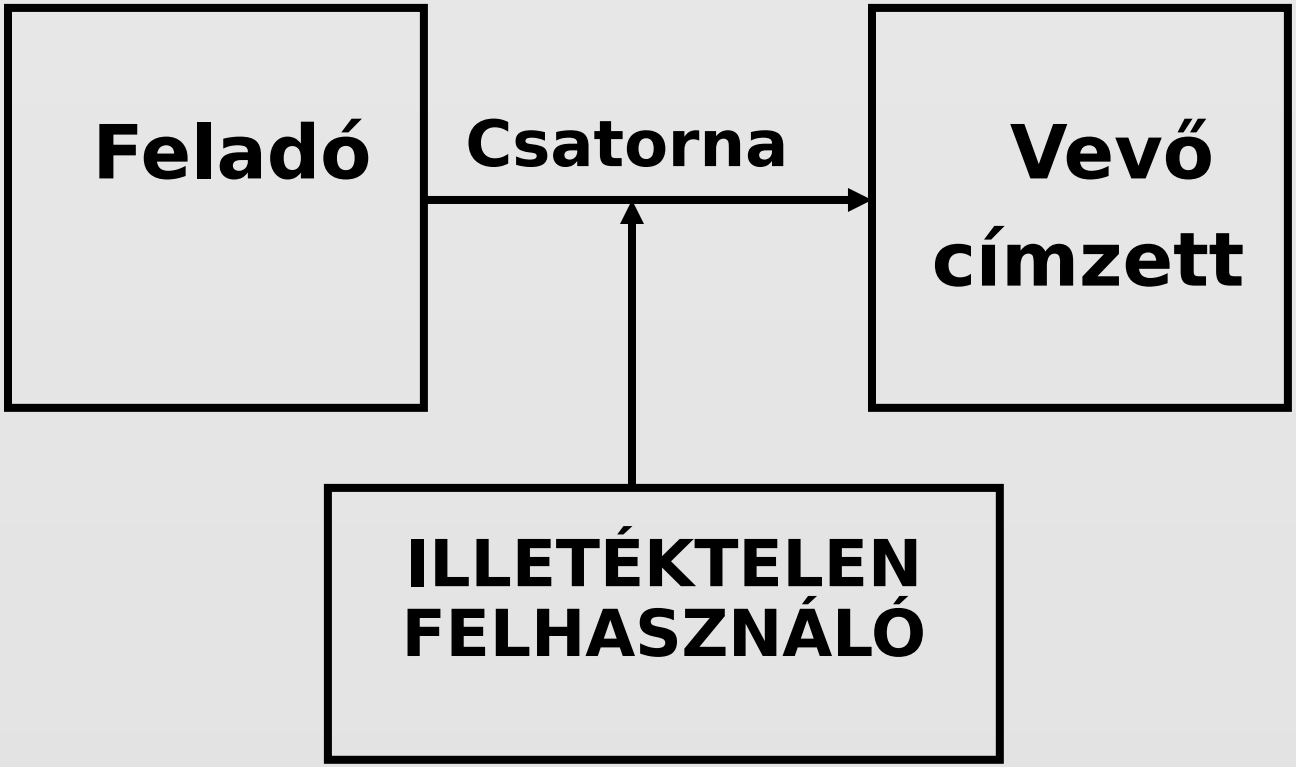
A kriptográfia fogalma

- A **kriptográfia** görög eredetű szó. Egy mára önállóvá vált, erősen matematikai jelleget kapott, interdiszciplináris jellegű, de elsősorban informatikai tudományág, amely a rejtjelezéssel, titkosírásokkal, kódolással; azok előállításával és megfejtésével foglalkozik.
- Adatok, üzenetek, rejtjelezésével – kódolásával foglalkozó tudomány.

A kriptográfia története

- **Ókor:**
- **Szteganográfia:** az üzenet elrejtése
- **Kriptográfia**: Az üzenet tartalmának, jelentésének elrejtése, kódolása. Átrendezés, behelyettesítés, Monoalfabetikus kódok: Káma-szútra módszer, Atbas, Polübiosz-négyzet, Caesar-rejtjel, kulcsszavas Caesar titkosítás
- **Középkor**: Grand chiffre kódja Vigenère-kód
- **Újkor:** Poligrafikus helyettesítő rejtjelek, Playfair-kód, Zrínyi Miklós titkosírása, Bacon titkosírása, könyvkódok
- **Egyszeri kulcsos titkosítás:** Cardano, Pázmány Péter és I. Rákóczi György.
- **Távírókódok**: Chappe, Morse, távgépíró kód (ASCII-kód)
- **I. világháború:** ADFGVX-kód, javított Vigenére-kód
- **II. világháború:** navahó nyelv, titkosítógépek: enigma, Purple, Typex, SIGABA, Lorenz SZ40
- **Modern kor:** számítógépes kódolás, DES, RSA, PGP

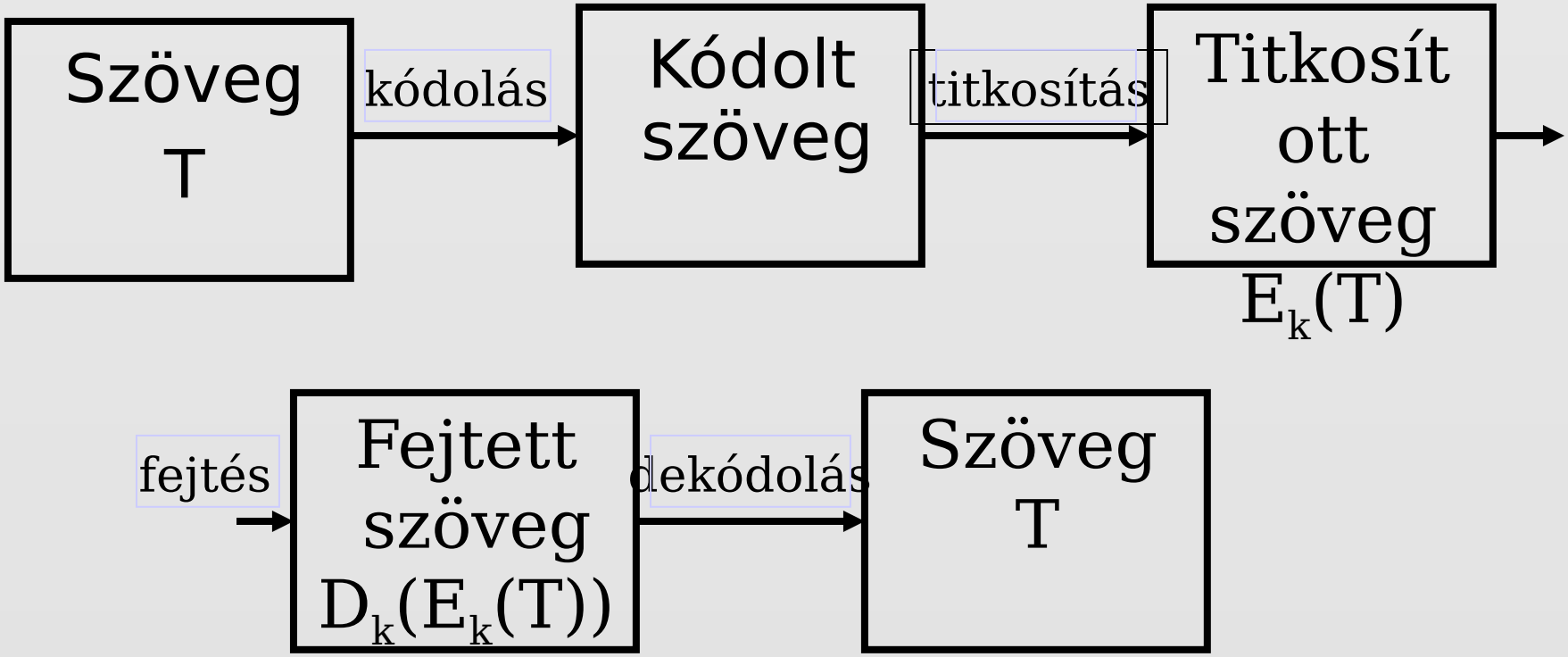
A kommunikáció folyamata



A kriptográfia részei

- Klasszikus kriptográfia: Régi korok titkosítása, statisztikai módszerekkel fejthető meg.
- Nyilvános kulcsú kriptográfia: modern technika, ismert módszer statisztikailag nem lehet megfejteni
- Bitsorozatokból, számokból áll
- Vegyes módon alkalmazva nagyon nehéz megfejteni

A szöveg útja



A jó titkosítás ismérvei

A XVII. században fogalmazta meg F. Bacon

- könnyű legyen a titkosított szöveg előállítása
- a fejtő kulcs ismeretében a fejtés könnyű legyen, fejtő kulcs hiányában a fejtés lehetetlen legyen.
- a titkosított szöveg legyen ártatlan kinézetű

Caesar féle titkosítás

(monoalfabetikus rendszerek)

A kulcsot az ábécé betűinek egy másik ábécével való helyettesítésével képezték, amelyet a nyílt ábécéhez viszonyítva három betűvel eltolnak.

Nyílt ábécé: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Rejtjel ábécé: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Példák a rejtjelezésre:

Miskolc: PLVNROF

Brutus: EUWXV

Caesar féle kulcsszavas titkosítás

Kulcsszó: KOMA

Nyílt ábécé: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Rejtjel ábécé: K O M A B C D E F G H I J K L N P Q R T U V W X Y Z

Példák:

Kartográfia: HKQTLDQKCFK

EGER: BDBQ

Polybios féle titkosítás

Polybios a harmadik pun háború nagy római hadvezérének Scipio Aemilianusnak volt a tanácsadója

	1 A	2 E	3 I	4 O	5 U
1 A	A	B	C	D	E
2 E	F	G	H	I	J
3 I	K	L	M	N	O
4 O	P	Q	R	S	T
5 U	U	V	X	Y	Z

Polybios féle titkosítás (példa)

Az ábécé betűit magánhangzó párokkal helyettesítjük, és észrevétlenül elrejtjük szavakban.

ITT ALUDT, AKI ELADOTT EGY UBORKAGYALUT. ITTHON CSÜCSÜLÖK.

Gyűjtsük páronként össze a szöveg magánhangzóit.

IA UA IE AO EU OA AU IO UU OU

Az elrejtett üzenet: KÜLDJ PÉNZT.

Egyéb titkosítási módszerek

- Hill módszer: mátrixokat használ
- Affin kriptorendszer

Polialfabetikus módszerek:

- Playfair módszer
- Kulcsszavas playfair módszer
- Blaise de Vigenére módszer
- Autoclave rendszer

Nyilvános kulcsú rendszerek:

- Knapsack (hátizsák) módszer

RSA algoritmus

1978-ban javasolt *R. Rivest, A. Shamir* és *L. Adleman* ezt a nyilvános kulcsú algoritmust, ami a szerzők neve alapján az *RSA* nevet kapta.

- Választunk véletlenszerűen két nagy p és q prímszámot. Ezek nagyságrendje legalább *100* decimális jegy.
- Kiszámítjuk: $n = p \cdot q$ modulust, és $\varphi(n) = (p-1)(q-1)$
- Választunk véletlenszerűen egy e számot $(e, p-1) = (e, q-1) = 1$ és $1 < e < \varphi(n)$
- Keresünk egy olyan d számot, amelyre fennáll az $e \cdot d \equiv 1 \pmod{\varphi(n)}$ és $1 < d < \varphi(n)$
- p, q és $\varphi(n)$ számokra továbbá nincs szükségünk.

Digitális aláírás

- A nyílt kulcsú titkosító rendszerek egy lehetősége, amellyel a hagyományos aláírást helyettesíthetjük az informatika világában.
- Igazolni tudjuk az aláíró személyét és azt, hogy a dokumentum az aláírás óta nem változott meg
- Jogszabályi alapja a 2001. évi XXXV törvény
- Jellemzői: technológiafüggetlen, könnyen létrehozható,

Összefoglalás

- A kriptográfia az emberi gondolkodás nagyszerű fejezete.
- Történelmi események és nagy gondolkodók formálták.
- A tudomány egy nagyon összetett és sok forrásból táplálkozó területe
- A kriptográfia évszázadokon keresztül tartó fejlődését a feltörhetetlen kód kidolgozása inspirálta
- A várt eredményt a XX. Században kidolgozott aszimmetrikus kulcsú titkosítással sikerült elérni, melynek képviselője az RSA módszer

KÖSZÖNÖM A MEGTISZTELŐ FIGYELMET!